

RECEIVED

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

APR 14 1998

FEDERAL COMMUNICATIONS COMMISSION
OFFICE OF THE SECRETARY

In the Matter of)	
)	
Implementation of the Telecommunications Act of)	CC Docket No. 96-115
1996;)	
)	
Telecommunications Carriers' Use of Customer)	
Proprietary Network Information and Other)	
Customer Information)	
)	
Implementation of the Non-Accounting Safeguards of)	
Sections 271 and 272 of the Communications Act of)	CC Docket No. 96-149
1934, as Amended)	

REPLY COMMENTS OF U S WEST, INC.

Kathryn Marie Krause
Suite 700
1020 19th Street, N.W.
Washington, DC 20036
(303) 672-2859

Attorney for

U S WEST, INC.

Of Counsel,
Dan L. Poole

April 14, 1998

TABLE OF CONTENTS

	<u>Page</u>
SUMMARY	ii
I. U S WEST SUPPORTS THOSE COMMENTORS OPPOSING ANY FURTHER COMMISSION RULES REGARDING END USER CUSTOMER PROPRIETARY NETWORK INFORMATION USE.....	1
II. U S WEST SUPPORTS THOSE COMMENTORS WHO ARGUE THAT NO IMPLEMENTING RULES REGARDING SECTION 222(b) ARE REQUIRED	5
III. THE FBI'S REQUEST REGARDING KEEPING CPNI ON SHORE.....	11
IV. MISCELLANEOUS.....	13
A. Omnipoint's Discussion of CPNI and Information Services Information	13
B. AICC's Arguments Regarding Internal Access Restrictions	15
V. CONCLUSION	19

SUMMARY

U S WEST herein comments on filings made with the Commission regarding its FNPRM in this docket.¹ We support those commentors who argue that no further rules are necessary with respect to Section 222 implementation or compliance. As the Commission noted in its CPNI Order, Congress created a statutory structure in which customer approval is inferred for Section 222(c)(1) uses of CPNI. As the overwhelming majority of commentors in this case persuasively argue, the Commission should defer to this Congressional model, leaving to businesses the handling of those idiosyncratic cases in which a customer might want to “restrict” his/her CPNI with respect to such uses.

Additionally, we support those commentors who assert that no further rules are necessary with respect to Sections 222(a) or (b). As the commentors persuasively argue, even those calling for additional “safeguards” in this area concede that the statute is clear on its face with respect to carriers’ obligations. To the extent a carrier violates the proscriptions of Sections 222(a) or (b), the Commission has existing and adequate enforcement powers to address such violation in a context which allows for a full airing of the facts and relevant defenses. The courts, as well, are available as enforcement authorities.

U S WEST supports those commentors arguing that the Commission should not enact rules along the lines suggested by the FBI. At this time, the FBI’s

¹ All acronyms or abbreviations used in this Summary are fully identified in the text.

proposal, as well as the FNPRM, are too lacking in detail to respond in other than the most general manner. And, to the extent that the FBI's proposal raises issues of international diplomacy involving other agencies, the issues proposed by the FBI should be vetted among these other administrative constituencies before any further action is taken.

Finally, we address the argument of Omnipoint that suggests that the Commission's proposal (which would allow end users to restrict the use of CPNI within the "total service relationship") would somehow implicate information generated from the ordering or provisioning of information services. We believe Omnipoint is incorrect. And, we address the arguments of AICC that LEC personnel engaged in alarm services offerings should be deprived access to all call detail CPNI, even in those cases where customer consent is inferred or has been affirmatively granted. We prove that, based on a factually incorrect assumption of AICC, its proposal is overbroad and would inappropriately burden LEC operations in a manner contemplated neither by the statute nor required by sound policy.

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

In the Matter of)	
)	
Implementation of the Telecommunications Act of 1996;)	CC Docket No. 96-115
)	
Telecommunications Carriers' Use of Customer)	
Proprietary Network Information and Other)	
Customer Information)	
)	
Implementation of the Non-Accounting Safeguards of)	
Sections 271 and 272 of the Communications Act of)	CC Docket No. 96-149
1934, as Amended)	

REPLY COMMENTS OF U S WEST, INC.

I. **U S WEST SUPPORTS THOSE COMMENTORS OPPOSING ANY FURTHER COMMISSION RULES REGARDING END USER CUSTOMER PROPRIETARY NETWORK INFORMATION USE**

U S WEST, Inc. ("U S WEST") supports those commentors arguing that the Federal Communications Commission ("Commission") should promulgate no further rules regarding the use of customer proprietary network information ("CPNI"), in those cases where Congress fashioned a statute that clearly permits such use, i.e., within the existing business relationship with respect to what the Commission has called the customer's "total service relationship."¹ Such commentors range from

¹ In the Matter of Implementation of the Telecommunications Act of 1996; Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information, CC Docket No. 96-115, Second Report and Order ("CPNI Order") and Further Notice of Proposed Rulemaking ("FNPRM"), CC Docket No. 96-115, FCC 98-27, rel. Feb. 26, 1998. Comments were filed Mar. 30, 1998.

local exchange carriers ("LEC")² to interexchange carriers ("IXC")³ to Commercial Mobile Radio Service ("CMRS")⁴ providers to Personal Communications Service ("PCS")⁵ providers. As those commentators point out, a restriction on the use of CPNI within the total service relationship would be contrary to the language of Section 222 and Congress' obvious intent to permit such use,⁶ contrary to Commission findings just recently made with respect to customer privacy expectations,⁷ and

² See Bell Atlantic Telephone Companies ("Bell Atlantic") at 1-3; BellSouth Corporation ("BellSouth") at 1-4; GTE Service Corporation ("GTE") at 1-4; Intermedia Communications Inc. ("Intermedia") at 3-7; SBC Communications Inc. ("SBC") generally; United States Telephone Association ("USTA") at 2-4.

³ See AT&T Corp. ("AT&T") generally; MCI Telecommunications Corporation ("MCI") at 2-6; Sprint Corporation ("Sprint") at 1-5.

⁴ See Vanguard Cellular Systems, Inc. ("Vanguard") at 3-6.

⁵ See Omnipoint Communications Inc. ("Omnipoint") at 1-3; Sprint Spectrum L.P. d/b/a Sprint PCS ("Sprint Spectrum") at 1-5.

⁶ See AT&T at 1, 4-5; Intermedia at 3-4; Vanguard at 3-4 (all citing to certain portions of the CPNI Order where the Commission was interpreting the statute and Congressional intent, specifically ¶ 37). And see, Intermedia at 6; MCI at 3; Omnipoint at 3; SBC at 2-5; Sprint at 2-3; Sprint Spectrum at 2-4; USTA at 3.

The Consumers' Utility Counsel Division of the Georgia Governor's Office of Consumer Affairs ("Georgia CUCD") is simply incorrect when it states that Congress "intended" that customers should have such ability (at 2), or "recognized" such an ability (at 4), or that the 1996 Act "indicates" such a Congressional intention (at 6). Furthermore, its general references to privacy surveys (at 4-5) are no more persuasive on the matter of consumers' privacy expectations in a commercial relationship than when cited by the Commission in its CPNI Order. See, e.g., ¶ 101.

⁷ See AT&T at 2, 6-7; Intermedia at 5; SBC at 5-6; Sprint at 4; Sprint Spectrum at 4-5; Vanguard at 5 (all asserting that customers expect to be kept informed by their carriers of products and services that might be of interest to them). And see MCI at 4 (depriving a carrier of access to CPNI will result in greater intrusions on customers' privacy); Bell Atlantic at 2; BellSouth at 3 and n.13 (both to the same effect).

contrary to the economic interests of consumers.⁸ Essentially, these commentators demonstrate that the Commission's proposal is unnecessary either as a matter of law or policy; and, as a matter of both, would be inappropriate.

Specifically, nothing about the language of Section 222(a) suggests that Congress -- through that subsection -- anticipated providing greater customer control over CPNI than Congress specifically outlined in Section 222(c). Section 222(a)'s general prescription regarding carriers' obligations to protect the confidentiality of proprietary information in their possession is just that -- a general statement of obligation and duty.⁹ A carrier might be held to violate that section, for example, if it did not protect the confidentiality of such information because it had lax security in either its systems or its information handling practices, or if it permitted an unauthorized disclosure of the proprietary information or if it used such information in a manner that might transgress Lanham Act proscriptions. But a carrier certainly does not violate Section 222(a) when it uses CPNI in the

⁸ See, e.g., AT&T at 6-7 (noting that deprivation of access to CPNI might result in a customer not having the benefit of a superior calling plan); Sprint at 5 (Commission's proposal would "severely limit the carrier's ability to efficiently market key services that may benefit the customer financially and in terms of convenience"); Sprint Spectrum at 4-5 (noting that deprivation of access to CPNI may result in customers being left out with respect to the delivery of commercial information that might be of benefit to them with respect to services to which they currently subscribe); Vanguard at 5 and n.10 (targeted marketing accomplished through CPNI benefits consumers by improving consumer awareness and service offerings).

⁹ See Omnipoint at 3 (describing this duty as a "very general provision" which "does not even use the term CPNI" and which refers to a carrier's "amorphous duty to protect the confidentiality of 'proprietary information'"); MCI at 2-3 (Section 222(a) is of a "general nature," enforced through the specific provisions of (b) and (c)), at 13

precise context in which Congress explicitly permitted such use and in which the Commission has stated Congress “inferred” customer approval.¹⁰

Furthermore, as a number of commentators point out, a customer need not restrict access or use of its CPNI to avoid unwanted telemarketing. Other legal protections are available to address this situation.¹¹ The access and use of information is something entirely independent of whether or not any specific individual wants to be communicated with over the telephone *via* a marketing contact. To the extent that individuals object to the latter practice, they currently have ample legal and regulatory protections through the application of the Telephone Consumer Protection Act of 1991 (“TCPA”).¹² Such protections actually provide customers concerned about “telephone solicitations” *per se* a much more targeted means by which to address their concerns -- concerns that may or may not be resolved through CPNI restrictions.¹³

(“a general provision, largely of a hortatory nature”); Sprint Spectrum at 3 (Section 222(a) imposes a “general obligation of confidentiality”).

¹⁰ See, e.g., CPNI Order ¶ 32. And see Sprint Spectrum at 3 (noting that the express, focused language of Section 222(c), operating as a “specific grant” must prevail over the “general obligation” of Section 222(a)); Intermedia at 4-5; Omnipoint at 3 (making the same point). And see AT&T at 5; MCI at 2-3 (Section 222(a)’s general obligations are enforced through the more specific pronouncements in subsections (b) and (c)); USTA at 3.

¹¹ See, e.g., AT&T at 2; Bell Atlantic at 2-3; BellSouth at 2-4 and n.11; GTE at 2-3; MCI at 4; SBC at 6-7; Sprint at 5.

¹² 47 U.S.C. § 227. And see Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991, 7 FCC Rcd. 8752 (1992); 47 C.F.R. § 64.1200.

¹³ See, e.g., BellSouth at 4; GTE at 2-3 (both pointing out that a restriction on marketing is a more ubiquitous mechanism to protect against marketing intrusions than a restriction on CPNI).

Finally, as SBC points out, not only has Congress spoken on the matter of CPNI use, it has done so in a manner that did not even invite Commission insinuation in the matter through a rulemaking.¹⁴ Given that none of the reasons the Commission previously proffered as requiring its intervention in this area exists with respect to the current issue, i.e., use of CPNI within a context which the Commission has already found Congress permitted, the Commission should demur and refrain from enacting any rules in this area.

II. U S WEST SUPPORTS THOSE COMMENTORS WHO ARGUE THAT NO IMPLEMENTING RULES REGARDING SECTION 222(b) ARE REQUIRED

U S WEST supports those commentors who argue that no implementing rules are necessary with respect to Section 222(b), since the statute is clear on its face.¹⁵ As with the other sections of Section 222, Congress did not invite the Commission to commence a rulemaking (or “establish a program”)¹⁶ on the language of the statute¹⁷ -- undoubtedly because of its clarity. Indeed, the Commission itself has observed

¹⁴ SBC at 7-8.

¹⁵ See, e.g., BellSouth at 4-5, 6; GTE at 4-5. Compare Telecommunications Resellers Association (“TRA”) at 3 (once again acknowledging the “straight forward” nature of the “directives” in Sections 222(a) and (b)), at 8 (describing Sections 222(a) and (b) as representing the adoption of “explicit safeguards for the competitively-sensitive data resale carriers must disclose to their network providers”), at 9 (“express safeguards” which are “remarkably clear and direct”).

In this Reply, U S WEST does not specifically rebut the assertions of TRA or its requests for relief. We find the recent TRA filing to add not much more than its previous filings. We believe we have sufficiently addressed the TRA position in our opening Comments (see U S WEST Comments at 7-13) and here cite to TRA only for certain specific propositions.

¹⁶ Sprint at 6.

that Section 222(b) amounts to an “express[] protect[ion].”¹⁸ Furthermore, the record demonstrates that adequate venues are available for enforcement of the obligations contained in that subsection.

No Commission “declaration,”¹⁹ “remind[er]”²⁰ or “teeth”²¹ are necessary regarding information obtained by LECs in the billing and collections context.²² Indeed, the record clearly demonstrates that issues associated with such contracts²³ are currently involved in litigation and have, in certain instances, been resolved in favor of IXC’s.²⁴

It is important to note that within the context of the FNPRM, the advocacy before the Commission just barely describes the nuances associated with end user CPNI *vis-a-vis* carrier information. While U S WEST will not here get into the legal arguments associated with the Pacific Bell situation,²⁵ Sprint’s own description of how such information can be both carrier information and CPNI belies the propriety

¹⁷ Compare SBC’s argument regarding the need for further rules regarding end user CPNI. SBC at 7-8. And see GTE at 6 (the Commission should allow the statute “to operate as a self-enforcing act of Congress”).

¹⁸ Sprint at 6, quoting from the FNPRM ¶ 206.

¹⁹ Sprint at 7, 9.

²⁰ MCI at 13.

²¹ TRA at 8.

²² See MCI at 7; Sprint at 7-8 (both referencing alleged LEC abuses of IXC billing and collections data).

²³ See MCI at 9 n.6, 16 (noting that often the use of information as between two carriers is addressed in contracts between those carriers).

²⁴ See MCI at 14 and n.10; Sprint at 7-8 and n.3.

²⁵ See MCI at id.; Sprint at id.

of a static regulatory mandate in this area.²⁶ As Sprint points out, certain data will -- at times -- be both carrier data and end user CPNI.²⁷ And, as Sprint concedes, in certain circumstances, an end user's authorization or approval will permit one carrier to access information involving that end user's relationship with another carrier.²⁸

Similar nuances are evident elsewhere. For example, MCI at one point argues that Section 222(a) would impose an obligation on carriers regarding "any confidential information that a carrier learns about another [carrier] from any source."²⁹ However, as U S WEST pointed out in our opening Comments,³⁰ and as MCI itself concedes,³¹ it is not sufficient to define the obligations of Section 222(a) in terms of the language of the duty alone (i.e., "a duty of confidentiality"). Rather, the duty only runs to "proprietary information."

²⁶ See Sprint at 8. And see MCI at 11 (discussing primary interexchange carrier ("PIC") designations, which are both carrier information and end user CPNI. The Commission should not venture into declarations about the PIC's categorization in this proceeding. The matter of passing PIC information between carriers for purposes of service initiation and transfer is currently being addressed in industry forums.).

²⁷ Sprint at 8.

²⁸ Id.

²⁹ MCI at 7, 8.

³⁰ U S WEST Comments at 7-8 and n.17.

³¹ MCI states that "As a practical matter, the . . . descriptions [in Section 222(a) and (b)] will probably cover about the same universe, since almost any proprietary information that one carrier learns about another is received or obtained from the other, as opposed to being the fruits of an independent investigation." MCI at 8. And see id. at 9 (referencing the securing of information from a "non-confidential source").

It cannot be said in the abstract that every bit of information Carrier A has in its possession which “relates to” Carrier B is proprietary, regardless of the source of the information, even if Carrier B might want the information to be treated “confidentially” and regardless of the “source” of the information. Thus, it would be totally inappropriate to create a presumption that Carrier A inappropriately used information (as proposed by MCI)³² or to impose strict liability (as proposed by TRA)³³ on a carrier for the use of information in the absence of proof that the information used was proprietary to the complaining carrier and was secured from that carrier.

The Commission should not try to predict all the circumstances in which these types of issues might arise. It should address them on a case-by-case basis, where the facts of each individual case can be addressed.³⁴ Proof that a “violation” of Section 222(b) has occurred rightfully is the obligation of Carrier B, who could determine whether inappropriate access and use occurred through a variety of available discovery mechanisms.

Certainly, the Commission should not approach the matter of Section 222(b) enforcement by undertaking management responsibilities, such as requiring

³² MCI at 12, 13.

³³ TRA at 13-15.

³⁴ As TRA points out, “[a]buse of carrier confidential data is nowhere near as rampant in the domestic, interexchange market as it was in the early to mid 1990s.” Id. at 4. At that time, there was no legislation. Now there is. Surely, the dwindling number of abuses, buttressed by the “straight forward directives” (id. at 3) in Section 222 render a formal Commission rule unnecessary.

training of employees³⁵ and mandating disciplinary processes.³⁶ As USTA points out “[b]etween the damage to a carrier’s reputation and the legal and business consequences associated with . . . a breach of trust [involving misuse of information], a carrier has substantial incentives to protect carrier, vendor and customer proprietary information.”³⁷ The fact that AT&T is alleged to have been unable to manage this issue in the past,³⁸ does not mean that an entire industry should be saddled by more regulation to implement a straight-forward statutory requirement.³⁹

Furthermore, while U S WEST cannot speak for all carriers, for carriers that have their operations organizationally focused on either retail or wholesale responsibilities (with the latter involving orders for resale and unbundled network elements (“UNE”), as well as the presubscription process), there is a sort of built-in protection against the inappropriate use of carrier information for marketing purposes.⁴⁰ Thus, contrary to the claims of some commentators,⁴¹ no additional

³⁵ See Sprint at 6-7.

³⁶ See *id.* at 7.

³⁷ USTA at 5. And compare MCI at 17 (arguing that such incentives clearly exist with respect to competitive carriers, but failing to explain why similar incentives do not also drive LEC behavior).

³⁸ TRA at 11.

³⁹ Had there actually been a statute in place during the time in which TRA asserts that AT&T mismanaged the process, the existence of a statute might well have resulted in more rigorous attention to the management of the situation.

⁴⁰ Intermedia acknowledges that some carrier operations reflect this type of internal division. Intermedia at 9. See also TRA at 10 (referencing carrier’s retail operations as somehow separate and apart from their wholesale operations).

safeguards are necessary.

The Commission should not promulgate a ubiquitous industry-wide rule in reaction to asserted inappropriate actions taken by some carriers. The enforcement process is the correct approach in which to proceed for such idiosyncratic types of actions⁴² -- a process which allows an affected carrier to explain its position, present a defense, and be controlled by the outcome.⁴³ The Commission's existing complaint

⁴¹ Intermedia at 7-8. The Commission need not "mandate that [incumbent LECs] ILECs maintain a bright-line separation between ILEC retail operations, wholesale operations, and their presubscription operations." *Id.* at 8-9. There is certainly nothing in the language of Section 222(b) which suggests a "firewall approach" (such as suggested by Intermedia at *id.*) or a "wall-off" of information (as suggested by TRA at 10) is required. *See also* TRA at 10-13. Rather, that subsection speaks directly to "uses." As the Commission found in its CPNI Order, there is a substantial and material difference between an access restriction (or, a "separations" of function approach, as suggested by Intermedia) and a "use" restriction. *See CPNI Order* at ¶¶ 65, 67, 195-197, 236. *And see* MCI at 16 (acknowledging the difference between "access" and "use" restrictions).

⁴² BellSouth at 3-4; GTE at 5; USTA at 5-6. *And see* MCI at 14 (noting that Section 201(b) liability would be available for alleged violations of Section 222(a) or (b)).

⁴³ For example, some carriers raise the issue of "winback" communications as representing inappropriate uses of carrier information. *See* Intermedia at 9-10; MCI at 15. The Commission just recently dealt with this issue within the context of end-user CPNI, there claiming that the use of the CPNI -- once the customer was gone -- was not appropriate because there were no longer services being subscribed to by the customer. *See CPNI Order* ¶ 98. It is true that if the Commission remains resolute with respect to this matter (which will undoubtedly be the subject of Petitions for Reconsideration), and depending on how it defines the "problem" associated with such communications, a potential use of the end-user's CPNI in a winback context might also implicate Section 222(b). *However*, it is equally true that a carrier could engage in a winback communication with the customer who has left without using the CPNI at all, by simply utilizing the name and address. Such would clearly not violate any Section 222 provision, including that pertaining to carrier information. (MCI is incorrect that only a non-LEC "learn[s] . . . information" associated with the need for a winback communication "because it will no longer be providing service." MCI at n.13. While the wholesale operations of a LEC learns that service is to be provided to another carrier and its customer on a date certain, the retail operations of the LEC also "learn[s] [that it is] no longer . . .

procedures and rules are quite sufficient to handle enforcement through the agency.⁴⁴ And, as is clear from the filed comments themselves, the courts also remain available as enforcement authorities.⁴⁵

III. THE FBI'S REQUEST REGARDING KEEPING CPNI ON SHORE

U S WEST agrees with those commentators who argue that the Federal Bureau of Investigation's ("FBI") entreaties to the Commission regarding the location of carrier CPNI are so lacking in detail with respect to the need for such a restriction,⁴⁶ that the Commission should decline to promulgate any kind of rule regarding the matter, at least at this time and in the context of a Section 222 rulemaking. As commentators point out, the FBI's proposal has nothing to do with Section 222 or Congressional intention.⁴⁷ Rather, the matter is totally independent of anything suggested by that Section and has the potential not just to protect customer privacy but to compromise it.⁴⁸

providing service" to a specific customer at some point. Id. A communication after learning of the second fact does not involve the use of carrier information and there is no "gap" regarding this situation that needs "plugg[ing]". Id. at 16. For these reasons, the Commission should engage in no further rules regarding winback communications.

⁴⁴ See note 42, supra.

⁴⁵ See note 24, supra.

⁴⁶ See, e.g., Omnipoint at 6 (the FBI's proposal and the FNPRM regarding the storage of CPNI lack sufficient details to comment on intelligently).

⁴⁷ See, e.g., id. at 7 (suggesting that Section 220 might be relevant, generally, to the discussion, but even that Section would not support granting the FBI's request); Iridium North America ("Iridium") at 2, 3-4 (noting that Section 222 has nothing to do with the FBI's proposal); GTE at 7-8; Intermedia at 11.

⁴⁸ See, e.g., Omnipoint at 7 and n.5 (noting the FBI wants the CPNI on shore so as to afford the FBI access for investigations). And see Iridium at 5; MCI at 18-20

It is also somewhat strange that the FBI would be advancing its position through the argument that domestic storage of CPNI will somehow advance the security precautions exercised by carriers with respect to CPNI.⁴⁹ It is almost intuitive, and is now part of the public record, that carriers have a strong business interest in protecting their information assets, including CPNI.⁵⁰ The Commission certainly need not grant the FBI the relief it requests to somehow advance or promote those security considerations.

We especially support the position of those commentators who suggest that the FBI's request implicates not merely domestic considerations but international ones, as well.⁵¹ Without a complete record on what those legal and policy implications are with respect to international and global networks,⁵² service provisioning to

(where MCI proposes that if accessibility to CPNI is the "key issue," then the "optimal solution" would be a requirement that all domestic CPNI be readily accessible from the United States. U S WEST urges the Commission not to make such a finding in this proceeding. It is impossible, given the state of the record at least thus far, to determine that MCI's solution is "optimal.").

⁴⁹ See GTE at n.10 (stating that the location of information does not automatically ensure its security, as demonstrated by a recent incident involving the Department of Defense).

⁵⁰ See, e.g., Ameritech at 2; MCI at 19.

⁵¹ See, e.g., Omnipoint at 8-9 and n.7.

⁵² See, e.g., Iridium at 7-9 (describing its network and billing systems and explaining how a CPNI "domestic storage only" requirement would be impossible for it to comply with, and expressing its belief that such would also be impossible for other U.S. carriers with global roaming capability); Ameritech generally (describing how certain work involving the development and implementation of information technologies might involve foreign "incidental access to CPNI"); Omnipoint at 8, 10. And see GTE at 7 (noting that the Internet makes obsolete the notion of a static place with respect to information storage); MCI at 17-19 (similar observation).

customers (which increasingly will become international and global),⁵³ as well as how other administrative agencies that might be impacted by Commission intervention in this area, the Commission should decline to become involved.

Finally, while the FBI's proposal does not -- on its face -- directly involve CALEA matters, CPNI does reflect transactional information. Any consideration of where such information should be stored, or how it should be accessed, should occur in a context involving law enforcement investigative authority.⁵⁴ It should not be confined to a docket involving primarily carriers and the implementation of a statute that never hints at the obligation the FBI seeks to have the Commission impose.

IV. MISCELLANEOUS

A. Omnipoint's Discussion of CPNI and Information Services Information

Omnipoint assumes, we believe incorrectly, that all information contained in an end user bill issued by a telecommunications carrier or incorporating telecommunications service information is CPNI,⁵⁵ and that an opt-out provision regarding to the use of CPNI within the total service relationship would "sweep in

⁵³ See, e.g., the discussion by Iridium of the commercial expectation regarding the "status" of a individual who enrolls for service in Germany. Iridium at 6. And see MCI at 18.

⁵⁴ See, e.g., Omnipoint at 6 (arguing that the FBI's arguments in support of its CPNI "domestic storage requirement" are similar to arguments it makes in the CALEA environment, and would amount to a wholesale change in existing legal requirements), 10-11.

⁵⁵ Omnipoint 3-4 (referring to this situation as being caused by a "statutory anomaly").

information service usage data that would not otherwise be part of CPNI.”⁵⁶

U S WEST is not certain how Omnipoint reaches this conclusion, even with respect to bundled offerings, since the statutory definition clearly confines its reach to the information contained in the bills “pertaining to telephone exchange service or telephone toll service.”⁵⁷

Parsing the argument, however, it seems that Omnipoint assumes that if a Personal Communications Service (“PCS”) package is billed in a bundled fashion, including enhanced services and other information services perhaps (such as a single billed amount of \$19.95 for all), that an “opt-out” provision extended to end users would allow them to prohibit the use of “total relationship” CPNI even for those purposes outlined in Sections 222(d)(1) and (2).⁵⁸ U S WEST does not read the Commission’s proposal, even at its most liberal, to suggest such a result.

Information associated with the provision of information (including enhanced services) is not CPNI.⁵⁹ While, as stated above, U S WEST supports those arguing that an “opt-out” right should not be extended to end users within the confines of the “total relationship” because such would clearly be contrary to expressed Congressional intent,⁶⁰ even if the Commission were to establish such a “right,” it would not preempt the carriers’ rights to use CPNI as provided for in Section

⁵⁶ Id. at 4.

⁵⁷ Id., citing to the statutory language.

⁵⁸ Id. at 4-5.

⁵⁹ See CPNI Order ¶ 46 and n.173.

⁶⁰ See Section I, supra.

222(d). Even more so, such action would not even extend to information that was not CPNI.⁶¹ With respect to such information, unless a carrier chooses voluntarily to allow a customer to restrict the use of such information in some fashion, neither Section 222 nor the Commission's proposal suggest any restriction in a carrier's use of the information.

B. AICC's Arguments Regarding Internal Access Restrictions

The Alarm Industry Communications Committee ("AICC") in its comments seeks "safeguards" regarding the use of data regarding alarm services providers that goes beyond that which the Commission has already established.⁶² Essentially, AICC wants the Commission to impose access restrictions on carriers' alarm monitoring personnel⁶³ with respect to all "call detail," rather than rely on the use restrictions the statute requires⁶⁴ and the Commission already has imposed.⁶⁵

⁶¹ Omnipoint suggests that because Section 222(d) "do[es] *not* permit use of CPNI for the same functions with respect to 'information services'" (at 5, italics in original), the Commission's proposals could somehow create a problem in using information services information for purposes similar to those outlined in Section 222(d)(1) and (2). However, because information services information is not CPNI in the first place, both the statute and the Commission's proposal are essentially silent with respect to the use of such information, not prohibitive of such use.

⁶² AICC at 2. And see In the Matter of Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information; Use of Data Regarding Alarm Monitoring Service Providers, Report and Order, 11 FCC Rcd. 9553 (1996) ("Alarm Order").

⁶³ AICC at 4-9.

⁶⁴ The "title" of Section 275(d) is "Use of Data."

⁶⁵ Alarm Order at 9557 ¶ 9 ("Section 275(d) restricts LEC personnel from using information regarding 'the occurrence or content of calls received by providers of alarm monitoring services' for the purpose of marketing their own alarm monitoring service, or an alarm monitoring service offered by another affiliated or unaffiliated entity."). AICC makes the fairly remarkable argument that its proposal should be

While AICC calls its proposal the “simplest and best method of ensuring” that LECs comply with the statute,⁶⁶ U S WEST points out below that such is far from the case. AICC’s erroneous factual assumptions and its overbroad proposal fails to appropriately reflect the statutory prohibition (i.e., a “use” restriction) and seek to impose burdensome, unwarranted regulatory obligations on LECs. Accordingly, AICC’s proposal should be rejected.

AICC repeatedly makes assertions suggesting that LECs record local calling information in a manner that creates “call detail” and allows them to “track” and create a list of those individuals calling alarm companies for service or utilizing their services. This assumption seems to append to both an administrative call between an end user and an alarm company (e.g., to the business office of such company to establish service or discuss billing) as well as to an “occurrence” call (e.g., a transmission from the customer premises through the phone line that an emergency event has occurred).⁶⁷ Based on this assumption, and because AICC

adopted since LECs have not proffered alternative proposals. AICC at 8-9. Since the Commission has not inquired about “alternative proposals,” there was clearly no requirement for LECs to proffer one. Until the Commission re-raises the matter, the resolution it reached in the Alarm Order is obviously the resolution.

⁶⁶ AICC at 7.

⁶⁷ Id. at 2 (“information concerning the occurrence or content of calls to alarm providers . . . will be contained in CPNI call detail records”), at 3 (“[a]larm monitoring data can be stored in any number of locations in a LEC’s records, including in individually-identifiable subscriber records constituting CPNI”), at 6 (records of alarm company customer premises testing “will be created a[t] regular intervals and included in customer CPNI call detail records;” “outbound call records will be created [in emergency events where a call is] trigger[ed] . . . to an alarm provider’s central station;” information associated with an outbound call will be recorded “in the records of each of [the alarm company’s] customers;” information “will be intermingled with other call records”), at 8 (“call detail records [are] most

believes that screening call detail associated with calls to alarm services providers and those to other destinations would prove too difficult, AICC proposes that LEC alarm monitoring personnel be deprived of all access to all end user call detail information.⁶⁸

AICC's proposal should be rejected in large part because its factual assumptions are incorrect. AICC would deprive LEC alarm monitoring personnel -- even when authorized under statute or by customer consent -- of all access to call detail information even though there is probably no alarm service call detail in the customers' records and even though what information might be there might not obviously be alarm service provider call termination information.

As a general matter (at least to the best of U S WEST's knowledge), LECs do not record local usage, in the absence of measured service offerings. Thus, as a general matter, with respect to "administrative type" calls to alarm services providers, there would be no end user call detail showing terminating calls to an alarm service provider.

Even in those cases where such dialing information is "recorded," however (i.e., in a measured service environment), it is not at all clear that a LEC's alarm monitoring personnel would even be aware that a recorded terminating telephone number was a competing alarm company.⁶⁹ But, even if the LEC personnel were

likely to contain information concerning the occurrence or contents of calls to alarm monitoring providers").

⁶⁸ Id. at 2, 6-7, 8.

⁶⁹ That is, while the information might meet the statutory definition of "alarm monitoring data," the LEC employee might have no knowledge that the information

aware of such a fact, to the extent that that information is not used to target a customer for alarm monitoring service, LEC personnel should not be deprived of access to the information.

With respect to “occurrence calls,” AICC also assumes incorrect facts with respect to the “recording” of such calls. With respect to most such calls, the call goes directly from the customer premises to the alarm company through “autodialer” or “digital dialer” technology.⁷⁰ This technology creates no LEC record of either the occurrence or the call. That is, the call is no different from any other local call with respect to the LEC network or recording functionality.

There are also alarm services that utilize private line services. With respect to these offerings (less than 5% of the service offerings), there also is no “recording” of the call generated by the alarm or emergency condition or occurrence.

Then there are alarm services utilizing derived channel technology. These services (along with wireless alarm services offerings) represent less than 5% of alarm services offerings. Of these derived channel offerings, the most well-known are Versanet and ScanAlert. With respect to Versanet offerings, the alarm company engages in all the monitoring and keeps all the records. It is only with respect to ScanAlert that a LEC creates records of the fact of a call and that the call was forwarded to the alarm company (i.e., basically an occurrence and time log).

constituted such data, knowing only that it represented a terminating telephone number. AICC seems to appreciate this, as it notes that a “screening” process would involve a LEC that is “compil[ing] the phone numbers used by alarm monitoring providers.” Id. at n.15.

Contrary to the suggestion of AICC, these types of records are not incorporated into Customer Service Records ("CSR"), where CPNI is generally located and accessed by marketing personnel. Rather, these records are created and maintained by a "network"-type organization.⁷¹ Given these facts, clearly a blanket access restriction on LEC personnel's access to call detail would be overbroad and overreaching.

Even AICC acknowledges that "if a LEC obtained customer approval to use CPNI for marketing purposes, that approval would *not* authorize the LEC to use information in that CPNI identifying 'the occurrence or contents of calls' to alarm monitoring providers for purposes of marketing an alarm monitoring service to the customer."⁷² Thus, even AICC notes the very limited restriction placed on LECs under the statute and acknowledges that it is a use restriction. Under the circumstances, it is clear that an access restriction would be inconsistent with the statutory obligation and would constitute an overbroad intrusion into the operations of LECs.

V. CONCLUSION

For all of the above reasons, the Commission need not promulgate further rules under Section 222(c)(1) dealing with internal use of CPNI within a "total

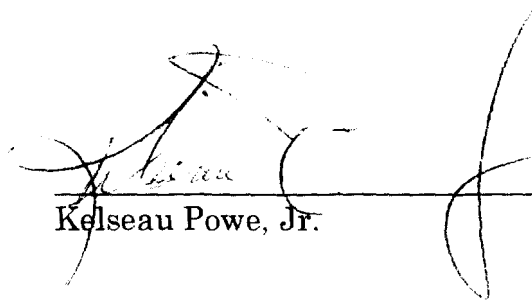
⁷⁰ U S WEST's understanding of the alarm services offerings is that 85% of alarm services penetration involves these types of offerings.

⁷¹ The records are maintained so that the network provider (i.e., U S WEST) can limit its liability to the alarm services company by demonstrating when it received an alarm and when it passed the information onto an alarm company.

⁷² AICC at 3 (*italics in original; underline added*).

CERTIFICATE OF SERVICE

I, Kelseau Powe, Jr., do hereby certify that on this 14th day of April, 1998, I have caused a copy of the foregoing **REPLY COMMENTS OF U S WEST, INC.** to be served, via first-class United States Mail, postage prepaid, upon the persons listed on the attached service list.



Kelseau Powe, Jr.

* Served via hand delivery

(CC96115g-cos/KK/ss)

*William E. Kennard
Federal Communications Commission
Room 814
1919 M Street, N.W.
Washington, DC 20554

*Gloria Tristani
Federal Communications Commission
Room 826
1919 M Street, N.W.
Washington, DC 20554

*Michael K. Powell
Federal Communications Commission
Room 844
1919 M Street, N.W.
Washington, DC 20554

*Harold Furchtgott-Roth
Federal Communications Commission
Room 802
1919 M Street, N.W.
Washington, DC 20554

*Susan P. Ness
Federal Communications Commission
Room 832
1919 M Street, N.W.
Washington, DC 20554

*A. Richard Metzger, Jr.
Federal Communications Commission
Room 500
1919 M Street, N.W.
Washington, DC 20554

*Carol Matthey
Federal Communications Commission
Room 544
1919 M Street, N.W.
Washington, DC 20554

*Janice M. Myles
Federal Communications Commission
Room 544
1919 M Street, N.W.
Washington, DC 20554

(Including 3 x 5 Diskette, with cover letter)

*Dorothy Attwood
Federal Communications Commission
Room 533-C
1919 M Street, N.W.
Washington, DC 20554

*Tonya Rutherford
Federal Communications Commission
Room 533-A
1919 M Street, N.W.
Washington, DC 20554